

Practitioner's Docket No. 57760/03-642

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Candella et al.

Application No.: 09/710,776

Group No.: 3621

Filed: 11/09/2000

Examiner: Elisca, Pierre E.

For: METHOD AND SYSTEM FOR DETECTING FRAUD IN NON-PERSONAL TRANSACTIONS

Mail Stop Appeal Briefs – Patents

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF  
(PATENT APPLICATION--37 C.F.R. § 41.37)

1. Transmitted herewith, in triplicate, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on June 15, 2005.
2. STATUS OF APPLICANT

This application is on behalf of a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10\*

(When using Express Mail, the Express Mail label number is *mandatory*;  
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

☒ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, Mail Stop Appeal Briefs- Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)

☐ with sufficient postage as first class mail.

37 C.F.R. § 1.10\*

☒ as "Express Mail Post Office to Addressee"

Mailing Label No. EV166756314US (mandatory)

TRANSMISSION

☐ facsimile transmitted to the Patent and Trademark Office, (703) \_\_\_\_\_ - \_\_\_\_\_

Signature

Date: August 15, 2005

Amy C. Walker

(type or print name of person certifying)

\* Only the date of filing (§ 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under § 1.8 continues to be taken into account in determining timeliness. See § 1.703(f). Consider "Express Mail Post Office to Addressee" (§ 1.10) or facsimile transmission (§ 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

a small entity \$250.00

**Appeal Brief fee due \$250.00**

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant petitions for an extension of time under 37 C.F.R. § 1.136 (fees: 37 C.F.R. § 1.17(a)(1)-(5)) for \_\_\_\_\_ month:

Fee: \$0.00

If an additional extension of time is required, please consider this a petition therefor.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee \$250.00

Extension fee (if any) \$0.00

**TOTAL FEE DUE \$250.00**

6. FEE PAYMENT

Authorization is hereby made to charge the amount of \$250.00 to the Credit Card as shown on the attached credit card information authorization form PTO-2038.

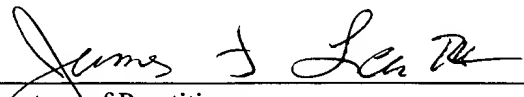
A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, please charge Deposit Account No. 06-540.

Date: 8-15-05

Reg. No.: 41,143  
Tel. No.: (918) 599-0621  
Customer No.: 22206

  
\_\_\_\_\_  
Signature of Practitioner  
James F. Lea III  
FELLERS, SNIDER, BLANKENSHIP,  
BAILEY & TIPENS, P.C.  
321 South Boston Ave., Suite 800  
Tulsa, Oklahoma 74103-3318

W324128



PATENT  
Attorney Docket No.: 57760/03-642  
Appellant's Brief (37 C.F.R. §41.37)  
USSN: 09/710,776  
Page 1 of 20

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Candella et al. )  
Serial No.: 09/710,776 )  
Filed: 11/09/2000 )  
Confirmation No.: 5507 )  
Title: METHOD AND SYSTEM FOR )  
DETECTING FRAUD IN NON- )  
PERSONAL TRANSACTIONS )  
Group No.: 3621 )  
Examiner: Elisca, Pierre E. )

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

APPELLANT'S BRIEF (37 C.F.R. §41.37)

Please be advised that this brief is in furtherance of the Notice of Appeal filed in this case on June 15, 2005. The fees required under § 41.20(b)(2) and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying Transmittal of Brief. In addition, a working copy is filed which is marked "APJ Copy".

This brief is submitted in triplicate.

\*\*\*\*\*

CERTIFICATE OF MAILING

I hereby certify that, on the date shown below, this correspondence is being deposited with the U.S. Postal Service in an envelope addressed to: Commissioner for Patents, Mail Stop Appeal Briefs - Patents, P.O. Box 1450, Alexandria, VA 22313-1450 as "Express Mail Post Office to Addressee" Mailing Label No. EV166756314US by Amy C. Walker.

Date: 8/15/2005

Signature: Amy C. Walker

08/17/2005 WABDELRI 00000004 09710776  
250.00 DP  
01 FC:2402

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. §41.37(c)):

- I Real Party in Interest
- II Related Appeals and Interferences
- III Status of Claims
- IV Status of Amendments
- V Summary of Claimed Subject Matter
- VI Grounds of Rejection to be Reviewed on Appeal
- VII Argument
- VIII Claims Appendix
- IX Evidence Appendix
- X Related Proceedings Appendix

**I. REAL PARTY IN INTEREST**

The real parties in interest in this case are:

George J. Candella  
348A Heritage Hills  
Somers, NY 10589

Irene H. Nohavec  
48 De Motte Avenue  
Clifton, NJ 07011

Michael L. Scrugggs  
2020 Longtail Trail  
Argyle, TX 76226

**II. RELATED APPEALS AND INTERFERENCES**

This application was appealed previously in an Appeal Brief filed July 12, 2004. The previous appeal resulted in the prosecution being reopened. The present appeal results therefrom. With respect to other matters that will directly affect, or be directly affected by, or

have a bearing on the Board's decision in this appeal, there are no such appeals or interferences or judicial proceedings known to Appellants, the Appellant's legal representative, or Assignee at this time.

### **III. STATUS OF CLAIMS**

Claims 1-32 were originally filed in the application on November 9, 2000. Claims 1-32 are pending in the application. The status of the claims in this application are:

Claims 1-32 stand rejected.

The claims on appeal are: Claims 1-32.

### **IV. STATUS OF AMENDMENTS**

No amendments were filed subsequent to the final rejection mailed April 8, 2005.

It is believed that all amendments, notices and briefs filed in U.S. Patent Application Serial No. 09/710,776 have been entered.

### **V. SUMMARY OF CLAIMED SUBJECT MATTER**

The claims involved in this appeal are directed to a method and system for detecting fraud in non-personal commerce transactions and reducing the risk and loss associated therewith.

Below, the appealed independent claim is reproduced wherein the appealed independent claim is read on the specification and drawings.

Claim	Subject Matter	Explanation	Specification Reference		Drawing Reference	
1.	Method for detecting fraud in non-personal transactions comprising the steps of:					
	collecting <b>purchaser data</b> for the transaction,		Page 7	Line 8, 12, 26	Character 110	FIG. 3
	said purchaser data comprising a <b>billing address</b>		Page 7	Line 25, 26, 29	Character 116	FIG. 3
	and a <b>ship-to address</b> ;		Page 7	Line 25	Character 118	FIG. 3
			8	21		
			9	29		
			10	2, 3		
			11	2, 4		
			8	1, 18, 25, 29		
			9	7, 23, 29, 30		

Claim	Subject Matter	Explanation	Specification Reference		Drawing Reference	
			Page	Line	Character	FIG.
	transmitting said ship-to address to a <b>fraud-detection system</b> ;		6	13,	100	2, 3
				16, 28		
			7	5, 11,		
				23		
			8	4		
	processing said ship-to address to determine whether the transaction is potentially fraudulent by checking the purchaser's ship-to address against criteria;		17	16		
	and returning the relative risks of fraudulent activity associated with the transaction.					

## **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

There is one (1) ground of rejection presented in this appeal. The following is a recitation of this ground of rejection.

1. Claims 1-32 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Tetro et al. (U.S. Patent No. 6,122,624), in view of Anderson et al. (U.S. Patent No. 5,884,289).

## **VII. ARGUMENT**

The Examiner rejects claims 1–32 as being unpatentable over Tetro et al. (U.S. Patent No. 6,122,624) in view of Anderson et al. (U.S. Patent No. 5,884,289). The Examiner's rejections are reproduced below:

As per claims 1, 14-16, 24-27, and 31 Tetro substantially discloses a method/ system for enhanced fraud detection in electronic purchase transactions from a remote site (which is readable as Applicant's claimed invention wherein it is stated that a method for detecting fraud non-personal transactions), comprising the steps of:

transmitting the purchaser's data to a fraud-detection system, the purchaser's data including a ship-to address for the transaction (see., abstract, specifically wherein it is stated that an electronic purchase is prompted to input the user's billing address and social security number, col 5, lines 47-59, the enhanced fraud detection system 10); processing the purchaser's data to determine whether the transaction is potentially fraudulent (see., abstract, specifically wherein it is stated that a determination is made whether the account associated with the social security number has been authorized for use, col 2, lines 39-61, please note that the process of matching the user's billing address and social security number is disclosed in the abstract, wherein said that a user at a remote terminal attempting to conduct an electronic purchase is prompted to input the user's billing address and social security number, where this information is used to verify the billing address of the user. Initially, the input social security

number is communicated to a local account database containing information about customers as identified by their social security number).

It is to be noted that Tetro fails to explicitly disclose the step of returning the relative risks of fraudulent activity associated with the transaction. However, Anderson discloses a computer based system that alerts financial institutions to undetected multiple debit card fraud conditions in their debit card bases by scanning and analyzing cardholder debit fraud information. The result of this analysis is the possible identification of cardholders who have been defrauded but have not yet realized it, so they are at risk of additional fraudulent transactions (see, abstract, col 4, lines 7-29). Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the fraud detection of Tetro by including the limitation detailed above as taught by Anderson because this would determine the dimension of fraud based on risk activity.

As per claims 2-6, 12, 18-22, 28, 30 Tetro discloses the claimed method wherein the processing step comprising parsing out the purchaser's ship-to address (see, abstract, col 39-61, specifically wherein it is stated that inputting the user's address).

As per claim 7, Tetro discloses the claimed method wherein the ship-to address checking step comprises checking the area code of the purchaser's phone number to determine if fits the geographic area of the ship-to address (see, abstract, col 39-61).

As per claims 8-11, 13, 23, 28, 29, Tetro discloses the claimed method wherein the ship-to address checking step comprises comparing the purchaser's ship-to address against the national of address service database or the publisher's change of address database (see, col 5, lines 61-67, col 6, lines 1-42, figs 2, 4, and 5, item 500).

As per claims 17, and 32 Tetro discloses the claimed method wherein the step of calculating comprising a score based at least in part upon the likelihood that the transaction is fraudulent (see, col 5, lines 47-60, please note that the step of calculating a score is equivalent a threshold check).

The Examiner further states in the Office Action mailed April 5, 2005 under the Response to Arguments section:

In response to Applicant's arguments, Applicant argues that the prior art of record (Tetro et al and Anderson) fail to anticipate or render obvious the recited feature:

a. "Collecting purchaser data for the transaction, said purchaser data comprising a billing address and a ship-to-address". However, the Examiner respectfully disagrees since Tetro discloses this assertion in the abstract, col 5, lines 5-67, col 6, lines 1-67. Please note that the home billing address at steps 214 and 216 is the same as a ship-to-address.

b. "checking the purchaser's ship-to-address against criteria". As indicated above, Tetro discloses in the abstract that a determination is made whether the account associated with the social security number has been authorized for use, col 2, lines 39-61, please note that the process of matching the user's billing address and social security number is also disclosed in the abstract, wherein said a user at a remote terminal attempting to conduct an electronic purchase is prompted to input the user's billing address and social security number, where this information is used to verify the billing address of the user. Initially, the input social security number is communicated to a local account database containing information about customers as identified by their social security number.

Applicant wishes to point out that the Examiner's referenced use by Tetro et al. of a "ship-to address" is, in fact, a reference to the billing address. In contrast, Applicants' invention includes the step of "checking the purchaser's ship-to address against criteria". Unlike Tetro et al., the claimed invention does not include a check step with regard to the "billing address". Further, the limitation, "collecting purchaser data for the transaction, said purchaser data comprising a billing address and a ship-to address" has been added to claim 1 to clarify that the "billing address" and the "ship-to address" are separate pieces of information.

Claim 1, as amended, is submitted to be patentable for at least the reason that neither Tetro et al. nor Anderson et al., either alone or in combination teach a method for detecting fraud that includes the step of processing a ship-to address to determine whether the transaction is potentially fraudulent by checking the purchase's ship-to address against criteria.

Dependent claims 3, 4, 6-10, 13, and 16-18 have been amended to properly reflect

antecedent basis with regard to amended claim 1.

Applicants respectfully disagree with the Examiner's assertion that Tetro et al. disclose a method/system comprising the steps of "transmitting the purchaser's data to a fraud-detection system, the purchaser's data including a ship-to-address for the transaction". The Examiner has noted correctly the teachings of Tetro et al. in the following sentence from the Office Action dated 04/08/2005: "[T]etro substantially discloses [collecting purchaser data for the transaction, said purchaser data comprising a billing address and a ship-to-address] in the abstract, col. 5, lines 5-67, col. 6, lines 1-67. Please note that the home billing address is the same as a ship-to-address." As can be appreciated, even though the ultimate destination may be the same, the "ship-to-address" is stored as a first piece of data while the "user's billing address" is stored as a second piece of data. Secondly in the case of fraud, the home billing address (cardholder's address) will likely never be the same as the "ship-to-address", i.e., a thief accessible location. The importance of separately tracking the ship-to-address and the user's billing address is highlighted in the Applicants' "Background of the Invention" beginning on page 2, line 22 through page 3, line 4 which states,

The electronic merchant receives an order from the person who gives a name, credit card number, and expiration date to the retailer in connection with a purchase. The purchaser directs that the merchandise be delivered to an address which is different than the credit card billing address. Using traditional methods, the merchant receives a credit card approval number from its gateway and ships the merchandise to the shipping address.

If, in fact, the credit card number has been stolen and the transaction is fraudulent, the true cardholder will likely reject the invoice when he is billed for

it, claiming fraud. Since the credit card company had confirmed the validity of the card (which remains in the owner's possession), and because the transaction is "card not present", i.e., was not involved with a signature verification, the credit card company has no liability. Assuming the cardholder refuses to pay the credit card company, the credit company will issue a charge back against the retailer, which has no recourse."

Transmitting the "ship-to address to a fraud-detection system, as is claimed in Applicants' novel method of claim 1, permits "checking the purchaser's ship-to address against a historical database to determine whether a pattern of fraudulent activity exists for the ship-to address; and checking the purchaser's ship-to address against a modeling engine to determine whether elements exist in the demographic data which correlate with fraudulent trends". (page 3, lines 21-26).

Checking the "ship-to address" provides benefits not available with other methods.

For example, if a merchant database reveals that there have been one or more deliveries to a specified ["ship-to"] address without objection by the cardholder, it is almost certain that further deliveries to that address (particularly if it matches the cardholder's address) are legitimate. If, however, a delivery is directed to an address inconsistent with the existing pattern associated with that critical purchase, it will trigger an alert that the transaction may be fraudulent. In such an event, the merchant will telephone or use the "safe-call" call verification program to communicate with the card owner to get confirmation of the bona fides of the transaction. (page 6, lines 13-27).

In conclusion, for at least the reasons set forth above, Applicants request allowance of amended independent claim 1 and claims 2 – 32 that depend, at least indirectly, therefrom.

Conclusion

For the reasons advanced above, Appellant respectfully contends that each claim is patentable. Therefore, reversal of all rejections is courteously solicited.

\* \* \* \* \*

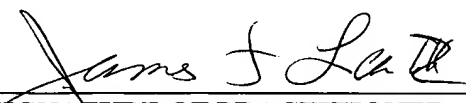
It is understood this paper is filed within the deadline set for response, however, please consider this paper to constitute a One Month Petition for Extension of Time should such be required. If any additional extension of time fee, or other fee is required by virtue of the filing of this paper, please consider this a general authorization to charge Deposit Account No. 06-0540 for the same; likewise instructions hold for any refunds or credits.

Respectfully submitted,

8-15-05  
\_\_\_\_\_  
DATE

Reg. No.: 41,143

Customer No.: 22206

  
\_\_\_\_\_  
SIGNATURE OF PRACTITIONER

James F. Lea III

FELLERS, SNIDER, BLANKENSHIP,  
BAILEY & TIPPENS, P.C.  
321 South Boston Ave., Suite 800  
Tulsa, Oklahoma 74103-3318  
Telephone No. (918) 599-0621

## VIII. CLAIMS APPENDIX

1. Method for detecting fraud in non-personal transactions comprising the steps of:  
  
collecting purchaser data for the transaction, said purchaser data comprising a billing address and a ship-to address;  
  
transmitting said ship-to address to a fraud-detection system;  
  
processing said ship-to address to determine whether the transaction is potentially fraudulent by checking the purchaser's ship-to address against criteria; and  
  
returning the relative risks of fraudulent activity associated with the transaction.
2. The fraud detection method according to claim 1, wherein the processing step comprising parsing out the purchaser's ship-to address.
3. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises a step of checking to determine whether the purchaser's ship-to address exists.
4. The fraud detection according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises comparing a zip code of the ship-to address against a post office database.

5. The fraud detection method according to claim 4, wherein the zip code is a ZIP + 4 zip code.
6. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises comparing the city and state of the ship-to address against the city and state with a ZIP + 4 code.
7. The fraud detection method according to claim 1 wherein the step of checking the purchaser's ship-to address against criteria comprises the area code of the purchaser's phone number to determine whether it fits the geographic area of the ship-to address.
8. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises comparing the purchaser's ship-to address against the national change of address service database or the publisher's change of address database.
9. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria comprises rating a building site associated with the "ship-to" address to determine whether the building or lot type is inconsistent with the transaction data.

10. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria further comprises the step of checking the purchaser's ship-to address against an historical database to determine whether a prior history of fraud exists.

11. The fraud detection method according to claim 10, wherein the prior history of fraud determining step comprises checking whether a record associated with the purchaser's ship-to address exists in the historical fraud database.

12. The fraud detection method according to claim 11, wherein the associated record is checked to determine whether negative data is associated with the ship-to address.

13. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria further comprises the step of checking the purchaser's ship-to address against an historical database to determine whether a pattern of fraudulent activity exists for the ship-to address.

14. The fraud detection method according to claim 13, wherein the pattern of fraud detecting step comprises determining whether an overlapping use of payment means and ship-to address is present by consulting a database of prior transactions.

15. The fraud detection method according to claim 13, wherein the pattern of fraud detecting step comprises retroactively notifying the merchant of previous transactions associated with the ship-to address once a pattern of fraudulent activity has been detected.

16. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria further comprises the step of checking the purchaser's ship-to address against a modeling engine to determine whether elements exist in the demographic data which correlate with fraudulent trends.

17. The fraud detection method according to claim 1, wherein the step of checking the purchaser's ship-to address against criteria further comprises the step of calculating a score based at least in part upon the likelihood that the transaction is fraudulent.

18. The fraud detection method according to claim 1, further comprising the step of checking to determine whether the purchaser's ship-to address exists.

19. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises comparing a zip code of the ship-to address against a post office database.

20. The fraud detection method according to claim 19, wherein the zip code is a ZIP + 4 zip code.

21. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises comparing the city and state of the ship-to address against the city and state with the ZIP + 4 code.

22. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises checking the area code of the purchaser's phone number to determine whether it fits the geographic area of the ship-to address.

23. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises comparing the purchaser's ship-to address against the national change of address service database or the publisher's change of address database.

24. The fraud detection method according to claim 18, wherein the ship-to address checking step comprises rating the building site associated with the "ship-to" address to determine whether the building or lot type is inconsistent with the transaction data.

25. The fraud detection method according to claim 18, further comprising the step of checking the purchaser's ship-to address against an historical database to determine

whether a prior history of fraud exists.

26. The fraud detection method according to claim 25, wherein the prior history of fraud determining step comprises checking whether a record associated with the purchaser's ship-to address exists in the historical fraud database.

27. The fraud detection method according to claim 26, wherein the associated record is checked to determine whether negative data is associated with the ship-to address.

28. The fraud detection method according to claim 25, further comprising the step of checking the purchaser's ship-to address against an historical database to determine whether a pattern of fraudulent activity exists for the ship-to address.

29. The fraud detection method according to claim 28, wherein the pattern of fraud detecting step comprises determining whether an overlapping use of payment means and ship-to address is present by consulting a database of prior transactions.

30. The fraud detection method according to claim 28, wherein the pattern of fraud detecting step comprises retroactively notifying the merchant of previous transactions associated with the ship-to address once a pattern of fraudulent activity has been detected.

31. The fraud detection method according to claim 28, further comprising the step of checking the purchaser's ship-to address against a modeling engine to determine whether elements exist in the demographic data which correlate with fraudulent trends.

32. The fraud detection method according to claim 31, further comprising the step of calculating a score based at least in part upon the likelihood that the transaction is fraudulent.

**IX. EVIDENCE APPENDIX**

None

**X. RELATED PROCEEDINGS APPENDIX**

No decisions have been rendered by a court or the Board in any proceeding identified pursuant to paragraph (c) (ii) of 37 CFR § 41.39.